Proceeding, Seminar Ilmiah Nasional Komputer dan Sistem Intelijen (KOMMIT 2008)
Auditorium Universitas Gunadarma, Depok, 20-21 Agustus 2008 ISSN : 1411-6286

MEMBANDINGKAN STEGANOGRAPHY DAN WATERMARKING PADA KEAMANAN FILE GRAFIK

Dwitya Putri[1], Aditya Kusuma[2], Nurul Hidayati[3], Jepri Torang[4], Yusak Tristanto[5]
I Wayan S. Wicaksana[6]

[1,2,3,4,5]Program Studi Teknik Informatika, Universitas)
[6]Pusat Studi Teknologi Sistem Informasi, Universitas Gunadarma.
[1]dwitya_putri@student .gunadarma.ac.id

ABSTRAK

Era globalisasi saat ini teknologi komputasi berkembang dengan pesatnya. Berkembangnya teknologi komputer dan informasi selalu memiliki dampak positif dan negative. Salah satu dampak negative yang terjadi adalah pencurian dan penyalahgunaan data digital, khususnya image. Dengan memanfaatkan kelemahan system penglihatan manusia, para penjahat digital melancarkan aksinya dan merugikan banyak pihak, bahkan mengancam keamanan sebuah Negara. Karena banyaknya kasus tersebut, dikembangkan teknologi untuk melindungi data digital (image). Salah satu teknologi itu adalah steganography dan watermarking. Paper kami membahas perbandingan hasil dari dua teknologi tersebut terhadap sebuah image JPEG. Parameternya adalah security (dengan transformasi DCT) dan kualitas gambar mencakup filterisasi, kontras gambar, cropping, resizing, rotation, dan enchancement. Untuk menguji parameter, kami menggunakan software WinWatermark V.2.2 YAG trial version dan Rea Watermark trial version dan untuk menguji parameter dengan metode steganography kami menggunakan software free Kamuflage. Hasil penelitian ini dapat dimanfaatkan untuk pengguna file grafik untuk memilih pendekatan atau aplikasi dalam melindungi file tersebut dari hal-hal yang tidak diinginkan.

Kata Kunci: grafik security, steganography, watermarking

1. PENDAHULUAN

Dunia teknologi komputer dan informasi berkembang sedemikian pesatnya. Semua ini berhubungan dengan jaringan global antar database. Adanya aplikasi untuk mencampur data digital yaitu musik, foto, dan video yang berbeda untuk berinteraksi dalam kapasitas informasi yang sangat besar (seperti e-commerce, e-business, e-learning). Salah satu dampak negative yang terjadi adalah pencurian dan penyalahgunaan data digital, khususnya image. Salah satu teknologi untuk mengatasi masalah itu adalah steganography dan watermarking.

Steganography adalah seni dan ilmu dari menulis pesan tersembunyi tanpa ada keterangan dari pengirim pesan hingga penerima pesan menyadari bahwa terdapat pesan tersembunyi. Digital watermarking adalah suatu sinyal permanent yang disisipkan ke dalam data digital (audio,video,image,dan text) yang dapat di deteksi oleh system computer dan di ekstrak nantinya. Teknik digital watermarking baik visible maupun invisible lebih kepada perlindungan hak cipta atau HAKI untuk kepentingan individu, meupun perusahaan bidang e-commerce untuk melindungi brand-nya. Digital watermarking sendiri terbagi menjadi 2 kategori utama yaitu visible dan invisible watermark.

Sebagai contoh, penelitian yang dilakukan oleh Poegoeh Joedhiawan dalam ITS community, melakukan penyembunyian informasi dengan metode *watermarking.* Metode ini menggunakan *transformasi wavelet*, *error correcting code*, dan memanfaatkan kelemahan system visual manusia. Sedangkan Yudi Prayudi menghasilkan skema keamanan pada citra *digital* dengan metode *watermarking visible* dan *invisible* pada *domain spectral* yang diterapkan dengan pendekatan *secure spread spectrum dan texture base.* Parameter yang digunakan adalah *PNSR, O, Corr,* dan *DVL* untuk membandingkan karakteristik dan efektifitas *watermarking*. Untuk contoh penelitian *Steganography* dilakukan oleh Niel Provos dan Peter Honeyman, mendeteksi *steganography* yang ada di internet yang diindikasikan sebagai alat komunikasi teroris via internet dengan menyisipkan pesan tersembunyi pada sebuah *image format* JPEG yang sering digunakan di dalam *Website* Internet. Niel dan Peter menggunakan transformasi DCT (*Discrete Cosine Transform*) menghitung kuantitas bit-bit *image* dimana pesan tersebut disembunyikan didalamnya.

2. PENDEKATAN

Steganography

Tujuan dari steganography dan cryptography sendiri adalah agar image tidak menarik perhatian pengunjung lain ataupun penerima image atau pesan itu sendiri. Tidak peduli seberapa kecilnya akibat dari enkripsi dalam sebuah Negara dimana enkripsi image adalah illegal. Sering kali steganography dan cryptography digunakan bersama untuk memastikan keamanan sebuah image. Steganograpy banyak digunakan di bidang security atau keamanan sebuah Negara, Seperti contoh kecil dalam cryptography adalah sebuah cincin alphabetic yang biasa terdapat dalam mainan anak-anak, dan terdapat surat yang berisi huruf-huruf alphabet. Triknya adalah dengan memutar satu arah sehingga alphabet tidak beradu :

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

S T U V W X Y Z A B C D E F G H I J K L M N O P Q R

Tentu saja sang penerima pesan harus mempunyai cincin alphabet ini agar dapt menerjemahkan pesan yang dikirimkan. Ini merupakan contoh kecil dan mudah dari steganography dan cryptography.

Deteksi dari paket steganography biasa disebut steganalisis dengan metode yang mudah yaitu dengan membandingkannya dengan pesan aslinya. Sebagai contoh dengan memindahkan hanya 2 bits dari setiap komponen warna dari image gelap atau dominant warna hitam dapat membuat 85 kali lebih terang dari

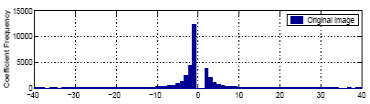
sebelumnya. Contoh selanjutnya 24bits bitmap mempunyai 8bits yang merepresentasikan tiga warna dari tiap bit pixel(merah,hijau dan biru biasa disebut RGB). Jika kita perhatikan hanya warna biru saja dimana biru mempunyai 28nilai(values) bit. Perbedaan antara 11111111 dan 11111110, dalam nilai intensitas biru mungkin tidak terdeteksi oleh system penglihatan manusia. Oleh karena itu dapat disisipkan pesan rahasia kedalamnya. Jika kita menggunakan warna hijau dan merah setiap 3 pixelnya maka dengan kode ASCII dapat dijadikan sebuah surat rahasia.

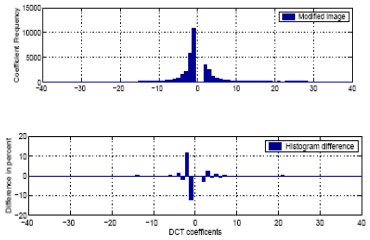
Informasi yang disembunyikan di JPEG

File ekstensi JPEG adalah yang paling banyak digunakan dalam dunia internet. Kami mendeteksi adanya steganography dalam internet dengan membandingkan file asli dan file kompresi seperti penelitian Neil Provos dan Peter Honeyman seperti gambar 1

Gambar 1. Contoh File Asli dan Kompresi

Image dengan resolusi 800x600 dan 24bit warna, sebelah atas adalah image asli tapi sebelah bawah sudah disisipkan kata-kata "Hunting of the Snark". Tetapi tidak ada perbedaan signifikan bila dilihat dengan system penglihatan manusia. Tanpa kompresi besarnya image 12Mb setelah dikompresi format JPEG ukuran file berubah menjadi 0.3Mb.Kami analisa dengan koefisien DCT dimana dalam histogram terdapat perbedaan signifikan seperti :





Gambar 2. Histogram Koefisien DCT

Menyisipkan sebuah image dalam file kompresi format JPEG mengubah koefisien DCT pada histogram.

Kita asumsikan X^2 adalah sebuah determinasi dari image yang menunjukkan distorsi dari penyisipan data. Karena test menggunakan stego analisis medium maka distribusi y^*i untuk X^2 test. Dengan n_i frekuensi dari koefisien DCT dalam image kita asumsikan image yang sudah disisipkan mempunyai frekuensi yang sama dengan koefisien DCT hasilnya fungsi aritmatik [6]

untuk mendeterminasi dibandingkan dengan

$$y_i = n_{2i}.$$

$$y_i^* = \frac{n_{2i} + n_{2i+1}}{2},$$

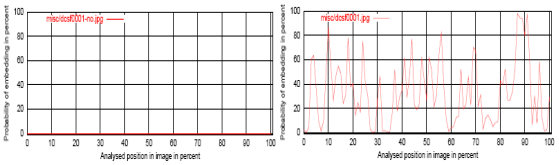
Nilai aritmatik X^2sebagai yang pembeda antara distribusi yang diberikan

$$\chi^2 = \sum_{i=1}^{\nu+1} \frac{(y_i - y_i^*)^2}{y_i^*}$$

Dimana v adalah derajat bebas nilai dari kategori yang berbeda dalam histogram minus satu. Kemungkinan dari penyisipan nilai p sebuah image yang diberikan komplement dari fungsi kumulatif distribusi

$$p = 1 - \int_0^{\chi^2} \frac{t^{(\nu-2)/2} e^{-t/2}}{2^{\nu/2}\Gamma(\nu/2)} dt$$

Dimana r adalah fungsi euler gamma. Kita dapat melakukan perhitungan penyisipan data dari area yang berbeda pada sebuah image.



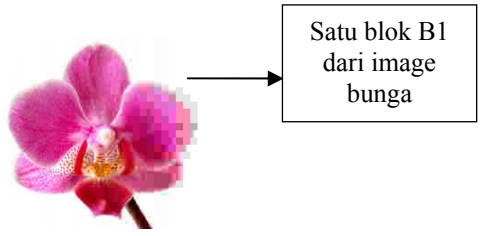
Gambar 3. Grafik Perbandingan Image Asli dan Modifikasi

Graf yang di atas menunjukkan hasil dari image yang tidak dimodifikasi. Sedangkan graf di bawahnya menunjukkan image yang sudah dimodifikasi. Kita dapat melakukan perhitungan penyisipan data dari area yang berbeda pada sebuah image. Dari sini kita dapat mengetahui system steganography yang digunakan. Untuk image yang tidak mengandung data tersembunyi pasti akan terlihat graf kosong atau perhitungan dengan nilai nol.

Sekuritas dari watermarking

Sekuritas dari watermarking dengan DCT (*Discrete Cosine Transform*) yaitu dengan melihat efektifitas dari algoritmanya. Efektifitas algoritma watermarking tidak dapat diasumsikan bahwa tidak mungkin penjahat tidak mengetahui adanya penyisipan watermarking dalam sebuah image (Swanson et al, 1998). Kekuatan sebuah produk komersial terletak pada sebuah asumsi.

Pointnya adalah membuat teknik yang sangat kuat dan membuat penyisipan algoritma ke public, yang biasanya menimbulkan kompleksitas komputasional dari penjahat untuk menghapus watermark. Beberapa menggunakan teknik orisinal image yang tidak ditandai dalam proses ekstrasi. Mereka menggunakan kunci rahasia sebagai fungsi keamanan dari watermarking. Sebagai contoh kita representasikan sebuah blok image bunga 8x8:



Gambar 4. Contoh Gambar Cuplikan

$$B_1 = \begin{bmatrix} 0.7232 & 0.8245 & 0.6599 & 0.7232 & 0.6003 & 0.6122 & 0.6122 & 0.5880 \\ 0.7745 & 0.7745 & 0.7745 & 0.7025 & 0.7745 & 0.7025 & 0.7745 & 0.7025 \\ 0.7745 & 0.7745 & 0.7025 & 0.7745 & 0.7745 & 0.7025 & 0.7025 & 0.7025 \\ 0.7025 & 0.7025 & 0.7025 & 0.7025 & 0.7025 & 0.7745 & 0.7025 & 0.7025 \\ 0.7745 & 0.7025 & 0.7745 & 0.7025 & 0.7025 & 0.7025 & 0.7025 & 0.7025 \\ 0.7025 & 0.7025 & 0.7025 & 0.7745 & 0.7025 & 0.7745 & 0.7025 & 0.7025 \\ 0.7025 & 0.7745 & 0.7025 & 0.7025 & 0.7745 & 0.7025 & 0.7745 & 0.7025 \\ 0.7025 & 0.7025 & 0.7745 & 0.7745 & 0.7745 & 0.7025 & 0.7025 & 0.7025 \end{bmatrix}$$

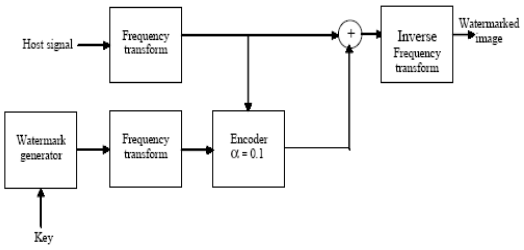
Perubahan yang terjadi dengan menggunakan DCT :

$$DCT(B_1) = \begin{bmatrix} 5.7656 & 0.1162 & -0.0379 & 0.0161 & -0.0093 & -0.0032 & -0.0472 & -0.0070 \\ -0.0526 & 0.1157 & 0.0645 & 0.0104 & -0.0137 & -0.0114 & -0.0415 & -0.0336 \\ -0.0354 & 0.0739 & -0.0136 & -0.0410 & -0.0081 & -0.0187 & -0.0871 & 0.0063 \\ -0.0953 & 0.0436 & 0.0379 & -0.0090 & -0.0394 & 0.0182 & -0.0031 & -0.0589 \\ -0.1066 & 0.0500 & 0.0034 & -0.0355 & -0.0093 & 0.0147 & 0.0526 & -0.0278 \\ -0.0790 & -0.0064 & 0.0088 & 0.0240 & -0.0200 & -0.0361 & -0.0586 & -0.0731 \\ -0.0422 & 0.0366 & -0.0460 & -0.0150 & 0.0518 & 0.0141 & 0.0105 & -0.0980 \\ 0.0025 & 0.0697 & 0.0327 & -0.0140 & 0.0286 & -0.0084 & -0.0422 & 0.0329 \end{bmatrix}$$

Dengan menggunakan Koefisien DCT =5.7656 gambar bunga mengalami perubahan watermark: Dimana kunci watermark adalah beberapa nomor acak sebagai berikut :

$$W = \begin{bmatrix} 1.6505 & 0.2759 & -0.8579 & -1.6130 & -1.0693 & 0.2259 & -0.4570 & 0.7167 \\ 0.7922 & -0.6320 & 0.8350 & -0.3888 & 0.4993 & 0.2174 & -1.6095 & -0.9269 \\ 0.7319 & 0.7000 & 1.6191 & -0.0870 & 0.7859 & 0.1870 & -0.3633 & 2.5061 \\ 0.9424 & 0.8966 & -0.0246 & -1.4165 & 0.5422 & 0.1539 & -1.1958 & 0.0374 \\ 0.2059 & 1.8204 & 0.5224 & -0.9099 & -1.6061 & -0.7764 & -0.8054 & -1.0894 \\ -0.1303 & -0.3008 & 1.6732 & -1.1281 & -0.3946 & 0.8294 & -0.0007 & -0.7952 \\ 0.0509 & -1.7409 & 1.1233 & 0.3541 & 0.1994 & -0.0855 & 0.1278 & -0.6312 \\ -0.1033 & -1.7087 & 0.5532 & 0.2068 & 2.5359 & 1.7004 & -0.6811 & -0.7771 \end{bmatrix}$$

Diagram proses watermarking dalam 1 blok image:



Gambar 5. Proses Watermarking

Maka hasil gabungannya adalah

$$DCT(W) = \begin{bmatrix} 0.2390 & 1.5861 & 0.1714 & 0.7187 & -0.3163 & -1.0925 & 2.6675 & 1.3164 \\ 0.1255 & 0.8694 & 2.8606 & -0.2411 & 0.6162 & -1.1665 & -0.1335 & -0.8266 \\ 0.0217 & -1.4093 & -1.3448 & 1.3837 & 1.3513 & 1.0022 & 0.8743 & 0.3735 \\ -1.7482 & 0.8337 & 1.5394 & -0.0076 & -1.7946 & 1.1027 & -0.4434 & -0.5771 \\ -0.7653 & 0.5313 & 0.9799 & 1.2930 & -0.0309 & -0.9858 & -0.9079 & -0.8152 \\ 0.4222 & -0.9041 & 1.2626 & -0.0979 & 0.6200 & 0.1858 & -0.1021 & 0.1452 \\ 1.4724 & -1.1217 & 0.7449 & -0.2921 & -0.3144 & -0.7244 & 0.4119 & 0.0535 \\ 0.4453 & 0.0380 & 0.9942 & -1.5048 & 0.0656 & 0.4169 & -0.7046 & -0.5278 \end{bmatrix}$$

Diagram blok menunjukkan:

$$f_w = f + \square\square \cdot w \cdot f$$

dimana f adalah koefisien DCT dari sinyal utama, Watermark sintyal adalah W dan $\square$ adalah energi watermarking yang nilainya 0.1

(□=0.1). Nilai DC dari sinyal utama tidak dimodifikasi. Untuk meminimisasi distorsi dari image yang sudah di watermark. Untuk itu nilai DC tetap tidak di watermark. Dimana ditulis dalam format matrik

$$DCT(B1w \begin{cases} DCT(B1) + \alpha.DCT(w). \\ DCT(B1) \text{ untuk semua} \\ \text{koefisien kecuali nilai} \\ \\ DCT(B1) \\ \text{untuk nilai} \end{cases}$$

Hasil dari perhitungan dimana $B1w$ adalah watermark sinyal dari $B1$

$$DCT(B_{1w}) = \begin{bmatrix} 5.7656 & 0.1346 & -0.0386 & 0.0172 & -0.0090 & -0.0028 & -0.0598 & -0.0079 \\ -0.0532 & 0.1258 & 0.0830 & 0.0101 & -0.0145 & -0.0101 & -0.0409 & -0.0308 \\ -0.0355 & 0.0635 & -0.0117 & -0.0467 & -0.0092 & -0.0206 & -0.0947 & 0.0066 \\ -0.0786 & 0.0472 & 0.0438 & -0.0090 & -0.0323 & 0.0202 & -0.0029 & -0.0555 \\ -0.0984 & 0.0527 & 0.0037 & -0.0400 & -0.0092 & 0.0132 & 0.0478 & -0.0255 \\ -0.0823 & -0.0058 & 0.0099 & 0.0238 & -0.0212 & -0.0368 & -0.0580 & -0.0742 \\ -0.0485 & 0.0325 & -0.0494 & -0.0146 & 0.0502 & 0.0131 & 0.0109 & -0.0985 \\ 0.0026 & 0.0700 & 0.0360 & -0.0119 & 0.0288 & -0.0088 & -0.0392 & 0.0312 \end{bmatrix}$$

Dimana nilai DC dari DCT($B1w$) sama dengan nilai DC dari DCT (B1). Untuk mengkonstruksi kembali image yang sudah di watermark, dengan invers dari DCT array dua dimensi yang diberikan :

$$B_{1w} = \begin{bmatrix} 0.7331 & 0.8361 & 0.6609 & 0.7228 & 0.5991 & 0.6026 & 0.6175 & 0.5922 \\ 0.7818 & 0.7809 & 0.7735 & 0.7011 & 0.7712 & 0.6955 & 0.7755 & 0.6998 \\ 0.7734 & 0.7746 & 0.6973 & 0.7682 & 0.7663 & 0.7002 & 0.6956 & 0.6920 \\ 0.7064 & 0.7093 & 0.7045 & 0.7037 & 0.7013 & 0.7692 & 0.6986 & 0.6933 \\ 0.7872 & 0.7100 & 0.7789 & 0.7081 & 0.7067 & 0.7012 & 0.7013 & 0.6996 \\ 0.7051 & 0.7032 & 0.7026 & 0.7801 & 0.7078 & 0.7741 & 0.7015 & 0.6978 \\ 0.7017 & 0.7765 & 0.7002 & 0.7067 & 0.7765 & 0.7026 & 0.7736 & 0.6992 \\ 0.6877 & 0.7048 & 0.7712 & 0.7800 & 0.7793 & 0.7001 & 0.7044 & 0.6974 \end{bmatrix}$$

Sangat mudah membandingkan antara $B1w$ dan B1 dan terlihat modifikasi keduanya dengan watermark.

Konsep pada visible sendiri sangat simple yaitu seperti cap pos pada sebuah surat atau kertas. Contohnya visible watermarking adalah logo stasiun televisi pada pojok kiri atas layar televisi. Seperti contoh gambar di atas, merupakan visible watermark atau watermark yang dapat di lihat dari suatu kontes edit image photoshop untuk kategori devil. Image-image tersebut dilindungi hak ciptanya dengan watermark.

Sedangkan konsep dari invisible watermarking atau watermarking yang tak terlihat adalah mencoba menyembunyikan watermark dalam sebuah image agar tidak dapat di ubah struktur image tersebut oleh pihak yang merugikan dan tidak merusak kualitas dari image aslinya. Untuk yang satu ini, karakteristik dari system penglihatan manusia untuk melihat sebuah image sudah tereksploitasi dalam proses penyisipan watermark secara tidak langsung.

3. EVALUASI

Dalam test kelompok kami dengan software kamuflage membuat sebuah file format JPEG dengan metode steganography. Pertama-tama image di add dan disisipkan teks ataupun image untuk disembunyikan ke dalamnya. Set password untuk membuka dan mengedit image nantinya, kemudian pilihan format image dalam JPEG (size paling kecil 80kb), GIF(format file terkecil no.2 setelah JPG),BMP(lebih mudah di edit perpixelnya),TIF,PNG(untuk format networking atau jaringan),TGA(untuk format game). Konversi dan image steganography sudah tercipta dengan sofrtware kamuflage. Untuk masalah security atau keamanannya dalam steganography file yang sudah dikompresi dapat di buka tetapi tidak dapat di edit ataupun di capture dengan print screen, sehingga tidak dapat dimaipulasi oleh orang lain. Dengan password key dari user untuk membuka sebuah image, seandainya kita simpan dan seseorang mencoba mengambilnya maka file Corrupt. Software kamuflage sudah memenuhi standart syarat sebagai software steganography untuk free software. Robustness atau kekuatan dalam image menggunakan software kamuflage hamper sama dengan digital watermarking yaitu dapat diatur masalah *filterisasi*, kontras gambar, *cropping*, *resizing*, *rotation*, dan *enchancement (*penambahan-penambahan). Dalam software tidak terdapat pengaturan kontras hanya cropping, rezising, dan penambahan – penambahan lainnya.

Untuk metode watermarking, dengan software WinWatermark V.2.2 YAG *trial version* dan Rea Watermark *trial version* adalah software visible watermark Masalah **sekuritas atau keamanan** suatu image menggunakan system blok DCT dapat dilihat dari penjelasan di atas. Suatu image yang sudah di watermark tidak dapat di edit, copy ataupun capture. Watermark tersebut bersifat permanent dengan kunci yang hanya dimiliki oleh pemilik image. Bila image yang sudah di watermark di ubah (konfersi dari file JPEG ke BMP) maka akan mengubah struktur dari

bit-bit parity pixel dan algoritma DCTnya, sehingga image akan rusak atau tidak sesuai image aslinya. **Robustness** dalam image dari hasil tes kami menggunakan dua software tersebut untuk filterisasi gambar sangat baik. Pada software tidak terdapat pengaturan kontras yang biasanya terdapat pada software komersial (contohnya adobe photoshop),untuk resolusi kami membandingkan antara panjang dan lebar suatu image dalam satuan pixel, inch,cm, atau mm, ukuran resolusi dalam pixel/inch, Untuk resize image dengan enlarge atau reduce, output file format dalam JPG,BMP,TIF,PNG,GIF,PDF. Dengan nilai parameter dari kami sebanyak 70% untuk kedua software tersebut untuk robustness

4. KESIMPULAN

Semua format file dalam steganography pasti invisible atau tidak terlihat, seperti konsep dari steganography sendiri yaitu agar pesan di dalam image tidak terlihat atau terdeteksi oleh orang lain selain penerima pesan yang di maksud. Watermark harus tidak terlihat sehingga tidak berdampak pada kualitas dari data yang akan dilindungi, dengan kata lain pertahanan harus kuat dari perusakan atau pemanipulasian image oleh orang lain. Pada watermarking visible atau terlihat bertujuan untuk memperlihatkan identitas pemilik image.

Ada dua persyaratan penting dalam penyembunyian data yaitu proses tidak terlihat dan kekuatan dari sebuah image. Dengan software yang kami uji masing-masing memiliki kelebihan dan kekurangan tersendiri dari ke dua metode tersebut. Untuk Hidden data mempunyai keunggulan tidak kasat mata dan punya kelemahan bila di capture / screen shot tidak berlaku dan bila gambar di manipulasi maka data akan rusak. Untuk Visible data keunggulannya sulit dimanipulasi dan kelemahannya yaitu mengubah output image kita. Baik dengan metode steganography atau pada teknik digital watermarking baik visible maupun invisible mencoba menyembunyikan watermark dalam sebuah image agar tidak dapat di ubah struktur image tersebut oleh pihak yang merugikan. Dan lebih kepada perlindungan hak cipta atau HAKI untuk kepentingan individu, maupun perusahaan bidang lebih banyak digunakan dalam e-commerce untuk melindungi brand-nya.

5. DAFTAR PUSTAKA

[1]. "Cryptography For Dummies" www.dummies.com/register/ Cryptography.chm

[2]. "Hidding Data within Data", www.garykessler.net/library/steganography.html

[3]. "Hsu, C., & Wu, J. . Hidden digital watermarks in images", www.tsi.enst.fr/~maitre/tatouage//icip2000.html

[4]. *Neil F. Johnson.* Steganography. www.nfj@jjtc.com

[5]. "Steganography and Digital WatermarkingTechniques for Protection ofIntellectual Property"

[6]. "SteganographyFAQ", www.infosecwriters.com/text_resources/pdf/Steganography_AMangarae.pdf

[7]. "Watermarking & image protection on the web", http://www.science-art.com/image_protection.asp

[8]. www. idea-group.com